UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, Plaintiff,	)	
v.	)	Case No. 1:23-cr-00125-MHC-RGV
TEREZ MONTAVIOUS PIPPINS, Defendant.	)	

DEFENDANT'S MOTION TO SUPPRESS ALL EVIDENCE OBTAINED AS A RESULT OF USE OF AUTOMATED LICENSE PLATE READER TECHNOLOGY

COMES NOW the Defendant, Terez Pippins, by and through undersigned counsel, and pursuant to the Fourth and Sixth Amendments of the United States Constitution, hereby moves to suppress all evidence obtained in this case that was the result of the warrantless search and review of Flock Safety automated license plate reader technology. In support whereof, he shows the following:

Discovery in this case shows that agents accessed Flock Safety automated license plate reader technology to scan for vehicles in the area of 2555 Stanford Drive on February 20, 2023. Agents assert that the cameras showed a white Nissan Maxima in the area for approximately six minutes on the night of a suspected drug transaction. The government asserts that Mr. Pippins was the driver of the vehicle. It is anticipated that the government will attempt to use this information at Mr. Pippins' trial. Because the evidence was obtained without a warrant, this evidence

should be suppressed.

I. ARGUMENT AND CITATION TO AUTHORITY

A. ALPR systems across the country collect and store massive amounts of data that can be used to identify and track drivers.

ALPRs are computer-controlled camera systems—generally mounted on vehicles or on fixed objects such as light poles—that automatically capture images of every license plate that comes into view. ALPRs can detect when a license plate enters the camera's field, capture a photograph of the car and its surroundings (including the plate), capture an infrared image of the plate at night, and convert the image of the plate into alphanumeric data—in effect "reading" the plate. ALPRs record data on every plate they scan, including plate number and precise time, date, and place it was encountered, uploading this data to a central database almost immediately after the scan. ALPR systems record extremely detailed GPS coordinates for each plate scanned. These coordinates are accurate enough to record the ALPR camera's location to a distance of two to four inches and within feet of the vehicle whose plate was scanned. The images captured by the systems can reveal not just the plate itself, but also the vehicle's occupants.[1] By design, ALPR collection is indiscriminate. ALPR operators turn on vehicle-mounted ALPRs at the start of

[1] Electronic Frontier Foundation, "Automated License Plate Readers" https://www.eff.org/pages/automated-license-plate-readers-alpr (last visited August 01, 2021)

their shifts, and the devices scan plates continuously until operators turn off the system at the end of their shift. Fixed ALPRs have a continuous connection to an ALPR server. Vehicle plates are scanned not just while cars are in motion or parked on public roads, but also while they are parked in privately owned parking lots, on private streets, and driveways of homes.[2]

B. Reviewing collected ALPR data constitutes a Fourth Amendment "search."

The agents' review of the data collected by the ALPR system in this case constituted a search for Fourth Amendment purposes.

Nearly fifty years ago, the Supreme Court held that "the physical characteristics of an automobile and its use generally result in a lessened expectation of privacy" because "[a] car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view." *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974). Generally, a person lacks a reasonable expectation of privacy in information he has voluntarily disclosed to a third party. *United States v. Miller*, 425 U.S. 435, 443 (1976). This principle is called the third-party doctrine. At that time, the Court decided these cases LPR technology was not

[2] Kaveh Waddell, How License-Plate Readers Have Helped Police and Lenders Target the Poor, The Atlantic (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-platereaders-have-helped-police-and-lenders-target-the-poor/479436 (last visited August 01, 2021).

contemplated or being utilized by law enforcement.

The United States Supreme Court recently clarified, however, that while individuals may have lessened expectations of privacy in certain information they reveal publicly, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018); *United States v. Jones*, 565 U.S. 400 (2012). As recognized by five concurring Justices in *Jones* and reaffirmed by the majority in *Carpenter*, "individuals have a reasonable expectation of privacy in the whole of their physical movements" because of the "privacies of life" those movements can reveal. *Carpenter*, 138 S. Ct. at 2217 (*citing Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id*. at 415 (Sotomayor, J., concurring)).

C. Searches of ALPR databases require a warrant.

Because ALPR data can reveal private and sensitive details about a person's life—details that individuals reasonably expect to remain private—warrantless searches of ALPR databases by law enforcement to find evidence of criminal activity are per se unreasonable. As the Supreme Court recently reiterated in *Carpenter*, warrantless searches "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" are typically unreasonable absent limited and specific exceptions. *Carpenter*, 138 S. Ct. at 2221 (*citing Vernonia School Dist. 47J v. Acton*,

515 U.S. 646, 652-53 (1995)). None of those exceptions apply here.[3]

In *United States v. Knotts*, 460 U.S. 276 (1983), the Supreme Court said that there is no reasonable expectation of privacy in public automobile travel, but noted that different constitutional principles may apply to dragnet-type law enforcement practices. *Knotts*, 460 U.S. at 284. Short-term monitoring of "a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." *United States v. Jones*, 565 U.S. 400, 430, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) (Alito, J., concurring). But society does not expect the government to engage in longer-term GPS monitoring, cataloguing every single movement of a person's car, to investigate most crimes. *Id.* This is especially so when location monitoring reveals "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Aggregating and then accessing even entirely public travel can invade a reasonable expectation of privacy in the whole of someone's physical movements. *Carpenter*, 138 S. Ct. at 2215, 2217, 2219.

As the Seventh Circuit Court of Appeals recently explained when addressing

[3] Notably, in *Jones* the Court did not apply the so-called automobile exception to justify warrantless tracking of the location of a car. See 565 U.S. at 410 n.7. *See also United States v. Katzin*, 732 F.3d 187, 204 (3d Cir. 2013) (holding that the automobile exception does not permit warrantless GPS tracking of a vehicle because the exception does not "permit [police] to leave behind an ever-watchful electronic sentinel in order to collect future evidence" based on the location of the car), rev'd en banc on other grounds, 769 F.3d 163 (3d Cir. 2014).

the use of pole cameras:

> In 1791, no one would expect—because the technology did not exist—that the government could capture a still (or moving) image of a citizen at a given time or place. Even once invented and introduced to society, few would have expected that the government would use then-unwieldy and expensive cameras to aid in fast-moving law enforcement investigations. Eventually, cameras grew so sophisticated, discrete, portable, and inexpensive that they pervaded society. By that point, the government's use of cameras was entirely unsurprising, even though the Framers might have balked at such a prospect when they penned the Fourth Amendment. See David Alan Sklansky, Too Much Information: How Not to Think About Privacy and the Fourth Amendment, 102 Cal. L. Rev. 1069, 1085 (2014) ("Cameras mounted in public and semi-public places ... are increasingly unremarkable, their presence taken for granted."). In other words, once society sparks the promethean fire—shifting its expectations in response to technological developments—the government receives license under current Fourth Amendment jurisprudence to act with greater constitutional impunity.
>
> Barring a transformation in governing law, we expect this chronicle of cameras to repeat itself again and again with the evolution of far more invasive technologies. Today's pole cameras will be tomorrow's body cameras, "protracted location tracking using [automatic license plate readers]," drones, facial recognition, Internet-of-Things and smart devices, and so much more that we cannot even begin to envision. New technologies of this sort will not disappear, nor will the complicated Fourth Amendment problems that accompany them. If anything, we should expect technology to continue to grow exponentially. And if current technologies are any indication, that technological growth will predictably have an inverse and inimical relationship with individual privacy from government intrusion, presenting serious concerns for Fourth Amendment protections.
>
> Assuming as much, it might soon be time to revisit the Fourth Amendment test established in *Katz*. . . Indeed, almost four decades ago, when considering a respondent's argument that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision," the Court reserved judgement because, "if such dragnet type law enforcement practices as respondent

> envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Knotts*, 460 U.S. at 283-84. As this case illustrates, round-the-clock surveillance for eighteen months is now unextraordinary.

United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).

Upon information and belief, the Flock ALPR system at issue scans all license plate that comes into the camera's view. The system also stores the data it collects so that it can be accessed at a later date. It is therefore possible for the government to track an individual's movement at all times through mobile and stationary ALPRs placed throughout the country and to preserve this data in readily searchable databases. The use of this information is not restricted in any way by law and it appears that officers are only accountable to their own police departments for misuse of the system. Although the Flock company may conduct audits of the system, there is no legal authority that governs the collection or use of the data. The idea that officers can access information about the movements of citizens at all times without the use of a warrant eliminates any Fourth Amendment protections that previously existed.

Here, unlike *Carpenter*, law enforcement did not seek or obtain any court process prior to searching the database. *See Carpenter*, 138 S. Ct. at 2221 (Government obtained Cell Site Location Information (CSLI) records pursuant to a court order issued under the Stored Communications Act, which required it to show "reasonable grounds" for believing that the records were "relevant and material to

an ongoing investigation").

ALPR data can be just as revealing as CSLI records, and therefore individuals maintain a similar reasonable expectation of privacy in it. For this reason, ALPR data should be subject to the same warrant requirement as CSLI. *Id*. at 2223.

The Supreme Court and the Eleventh Circuit have already metaphorically drawn a line in the sand regarding advancing technology and what information law enforcement may and may not access without a warrant. The Eleventh Circuit recently interpreted the *Carpenter* decision as holding "that the acquisition of historical cell-site records is a search under the Fourth Amendment, so the government must obtain a warrant to access such records." *United States v. Green*, 969 F. 3d 1194, 1206 (11th Cir. 2020). The deciding factor in *Carpenter* and in *Green* is the government's ability to obtain historical location data without a warrant. The aggregate collection of an individual's movement reveals details which individuals reasonably expect to remain private. Thus, warrantless searches of the ALPR databases are per se unreasonable.

D. State law requires individuals to obtain license plates in order to use vehicles and to travel on public roads, which makes the information at issue here significantly more concerning than the cell-site location information at issue in *Carpenter*.

Notably, unlike the cell-site location information at issue in *Carpenter*, individuals are required to have license plates by state law. State law requires that anyone driving a car must have a license plate. O.C.G.A. § 40-2-20(a)(1)(A)

("[E]very owner of a motor vehicle, including a tractor or motorcycle, and every owner of a trailer shall, during the owner's registration period in each year, register such vehicle . . .and obtain a license to operate it for the 12 month period.").

Moreover, Georgia state law requires that the tag be clearly displayed:

> [E]very vehicle required to be registered under this chapter, which is in use upon the highways, shall at all times display the license plate issued to the owner for such vehicle, and the plate shall be fastened to the rear of the vehicle in a position so as not to swing and shall be at all times plainly visible. . . . It shall be the duty of the operator of any vehicle to keep the license plate legible at all times. No license plate shall be covered with any material unless the material is colorless and transparent. No apparatus that obstructs or hinders the clear display and legibility of a license plate shall be attached to the rear of any motor vehicle required to be registered in the state. Any person who violates any provision of this Code section shall be guilty of a misdemeanor.

O.C.G.A. § 40-2-41.

Not having a tag puts an individual at risk of criminal sanctions and penalties. First, any person who fails to register is subject to criminal penalties: a conviction for a misdemeanor and a fine of up to $100.00. O.C.G.A. § 40-2-20(d). The failure to clearly display the license plate also results in a misdemeanor. O.C.G.A. § 40-2-41. Finally, not having a valid tag creates probable cause for the car to be stopped in Georgia. *See, e.g.*, *Caffee v. State*, 303 Ga. 557 (2018) (noting that officer stopped car for having an expired tag).

Further, nothing advises motorists of the type of surveillance they will be subjected to by virtue of having a license plate. Georgia state code requires that an

individual seeking a tag must meet certain standards, including that (1) they have the title for the car; (2) the vehicle is properly insured; (3) the car meets the relevant emissions standards; and (4) proof that all fees, permits, and taxes have been paid. O.C.G.A. § 40-2-29(a). Therefore, when an individual obtains a tag for their car, they understand that they are certifying that they meet the statutory provisions to obtain the tag. However, an individual obtaining the tag would not reasonably expect that government actors---whether state, federal, or local—would be able to track all of their movements in the way that was done here.

Carpenter also forecloses any argument that an individual has the option of simply choosing not to get a car. There, the Court rejected the third-party doctrine because "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." *Carpenter*, 138 S.Ct. at 2220. Here, obviously, the ability to travel on public roads and to use vehicles is plainly even more a "pervasive and insistent part of daily life" that is "indispensable to participation in modern society."

In sum, state law requires individuals to obtain and clearly display identifying information, without explaining to individuals that they will be unable to escape the pervasive tracking that private companies capture and then sell to law enforcement agencies. Meanwhile, there are no requirements for law enforcement agencies to obtain the information—no court order, no probable cause, not even reasonable

suspicion. This flies in the face of the Fourth Amendment. This Court should grant Mr. Pippins' motion and suppress this evidence.

E. CONCLUSION

The Fourth Amendment of the United States Constitution protects a person from unlawful searches and seizures. In filing this Motion, Mr. Pippins specifically moves to suppress all fruits obtained from the illegal searches and seizures, including all evidence obtained as a result of the unreasonable, unlawful, warrantless review of ALPR data in this case. *Wong Sun v. United States*, 371 U.S. 471, 487-488 (1963); *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).

Respectfully submitted this 29th day of November 2029.

s/Saraliene S. Durrett
SARALIENE S. DURRETT
GA Bar No. 837897
SARALIENE SMITH DURRETT, LLC
1800 Peachtree Street, Suite 300
Atlanta, GA 30309
(404) 433-0855
ssd@defendingatl.com